DEFENSE CONTRACT AUDIT AGENCY
DEPARTMENT OF DEFENSE
8725 JOHN J. KINGMAN ROAD, SUITE 2135
FORT BELVOIR, VA 22060-6219

IN REPLY REFER TO

19 September 2000

PAS 0-730.1 00-PAS-082(R)

MEMORANDUM FOR REGIONAL DIRECTORS, DCAA
DIRECTOR, FIELD DETACHMENT, DCAA

SUBJECT: Audit Guidance on Storage and Backup of Final Electronic Working Papers

SUMMARY

Recent reviews by Headquarters elements have demonstrated a need to require backup of final electronic working papers. Original working paper files are always at risk of being lost, damaged, or destroyed. This risk has been accepted because of the significant cost of duplicating and storing backup paper files, and the comparatively slight risk of loss. However, duplication and storage costs of electronic working papers are small, and there is the additional risk that the relatively smaller and more fragile electronic medium itself may degrade or be separately lost, damaged, or destroyed. This memorandum modifies current policy to require that FAOs develop and implement written procedures to maintain backup copies of all final electronic working papers for each completed audit.

GUIDANCE

In addition to the original electronic files stored with the official working paper file, FAOs which have not previously done so will prepare two backup copies of all final electronic working papers for each completed audit assignment. One backup, the “archive” copy, will be stored separately on removable media such as CD-ROM or diskette. The second backup, the “working” copy, should be commonly available for reference and may be stored on the FAO LAN or other accessible location. The "archive" backup copy should be maintained as long as the original copy. This “archive” backup should be stored separately from the original while both are kept at the FAO. When the original file is sent to storage the “archive” backup copy should be mounted in the file with the original copy. The "working" backup copy may be deleted when it is no longer needed for reference purposes. Each backup copy should be tested to ensure it can be unarchived and its contents read. Specific guidance for the use of Agency software and hardware during the backup procedure is enclosed (Enclosure).

Each FAO must develop written procedures to ensure all required final electronic working paper files are backed up and verified. Procedures should be tailored to the specific FAO organization, taking into consideration its hardware, software, and organizational structure. Written procedures should be completed by 31 December 2000.

FAO procedures should include the following elements:

- Creation of the two backup files as described above.
- Control use of the electronic files as follows:
  - ✓ "working" copy for routine unofficial purposes
  - ✓ original for official purposes and creation of new backups
  - ✓ "archive" copy for use only if the original becomes lost or damaged
- Verification that all three copies of electronic working papers may be opened and their contents read.
- Specific identification of the locations where the "working" and "archive" files will be stored.

REQUIRED ACTIONS

Each FAO will:

- Effective immediately:
  - ✓ create an "archive" backup copy of all final electronic working papers on removable media such as CD-ROM or diskette
  - ✓ verify that the "archive" file can be opened and its contents read
  - ✓ store "archive" file copy separately from the original, which should remain with the printed copy of the report and "hard copy" audit working papers
  - ✓ create a "working" backup copy of all final electronic working papers on a readily accessible location such as the FAO LAN, except for files determined in writing to require no further working papers access
- By no later than 31 December 2000, develop FAO specific written procedures to ensure final electronic working papers are backed up and that "working" copies are deleted when no longer needed.
- Coordinate any required hardware or software purchases with its region.
- Adjust written procedures as necessary for changes in guidance, software, hardware, and organizational structure.

CONCLUDING REMARKS

Field audit office personnel should direct questions regarding this memorandum to personnel in the regional office. If regional personnel are unable to answer or have questions of their own, they should contact Mr. Joseph A. Stewart, Program Manager, Auditing Standards Division at 703-767-3236, fax 703-767-3234, or e-mail dcaa-pas@dcaa.mil.

/s/

Lawrence P. Uhlfelder
Assistant Director
Policy and Plans

Enclosure
Guidance for FAO Electronic Working Paper Backup Procedures

DISTRIBUTION: C

Guidance for FAO Electronic Working Paper Backup Procedures

FAO procedures should include a combination of the APPS software, existing hardware, and adequately trained employees. FAOs have the flexibility to implement a backup procedure that reflects their office structure. This is critical because each office has a unique workflow process. The required archiving and backup process takes place at the very end of the audit process, i.e., the audit report has been signed and delivered to the customer. All the electronic working papers, including the capture of the e-mail transmittal receipt, can be included in the final archived/backed-up electronic working papers. The current version of APPS already has the capability to create these electronic backups.

APPS has two excellent features for backing up electronic working papers. APPS can generate a complete backup zip file or it can create a self-extracting executable file. Currently, the CAM already requires the official electronic files to be stored in the audit working paper package. FAOs are already using APPS to create a self-extracting file of the working papers in order to meet this CAM requirement. To make separate backups, prior to making the final archive file, end users need only select the backup function in APPS, and a zip file containing all the electronic files in the assignment folder will be created. Consequently, FAO backup procedures should include the following closing action steps:

[This process assumes a completed audit package - all working papers (including both paper and electronic) are complete, and the final report is issued.]

1. **The end user accesses the audit work paper files using APPS**. This could be any member of the DCAA work force. It is critical that whoever is assigned this responsibility be appropriately trained, including training in APPS.

2. **Select the *Admin Functions* within APPS**.

3. **Select *Daily Backup* to make first backup file (.ZIP), and save this to the LAN**. Each office should establish a LAN directory structure that fits their audit environment. For example, FAOs may set up separate directories by audit team, type of audit, or by contractor. This structure simply provides a means to better categorize and manage these completed audits. The purpose of this LAN-based storage is to provide immediate access to previously completed audits. It should be considered a temporary storage location.

Each FAO should set retention periods based on the nature and structure of the data. For instance, if structured by type of audit, one FAO might choose to keep proposal audits for six months, but incurred cost audits for 12 months. Once the designated time period has expired, simply delete the files. Storage time periods will also be impacted by the available amount of LAN storage space available for this purpose.

This use of the LAN as a temporary file library would provide every auditor access to historical files provided they have either direct LAN access or dial-in access to Memphis. Real-time on-line availability of audit files should increase productivity and reduce the occurrence of auditors accessing the "official" working paper electronic files, thus reducing the chance for accidental data loss.

4. **Select *Daily Backup* again to make second backup file (.ZIP), and save this to removable media such as CD-ROM, diskette, etc**. The auditor should follow the standard labeling practices described in CAM to properly identify (external) CD-ROMs and diskettes. The backup copy should be considered as the long-term backup and should be retained for the same time period as the original audit file. This long-term backup should be stored separately from the original while both are kept at the FAO. When the original file is sent to storage the long-term backup copy should be mounted in the file with the original copy.

Writing data to a CD-ROM is advantageous because of its increased storage space and longevity, which is greater than both the standard 1.44 MB diskette and the LS-120 SuperDisk. Also, at this time CD-ROMs have a cost advantage of about $1 per unit, compared to a $5-$8 unit cost for an LS-120 SuperDisk.

Creating backups using 1.44 MB diskettes should be avoided, if possible, unless the data will fit entirely on one diskette. Although the APPS backup procedure can backup/span data to multiple diskettes, the process of inserting and writing to successive diskettes is error prone. This occurs because the process of physically writing data to a diskette normally has not been completed when the software "says" to insert the next diskette. Consequently, a disk is often removed prematurely before all data has been successfully written to it. Thus, data is lost when the zip file's structure becomes corrupted and is unreadable. Further, this is not apparent until there is an attempt to unzip this critical data. Therefore, if a CD-ROM writer is not available, it is preferable to store work paper data files on LS-120 diskettes instead of 1.44 MB diskettes.

5. **Select the *Save As Archive,* and this will create the final official executable file (.exe) that is stored within the completed audit folder**. This folder contains, at a minimum, the hard copy documents as required by CAM 4-407c(8) and any other printed working papers. This official package should be protected physically, and generally should NOT be available to the work force. Any access to these official files must be restricted.

6. **Final Step**. Using another machine, verify that both files stored on the removable media in Steps 4 and 5 can be unarchived. This is a critically important safeguard/internal control task that must be performed. This is a simple test to ensure the official file and its primary backup was not corrupted during the generation process.